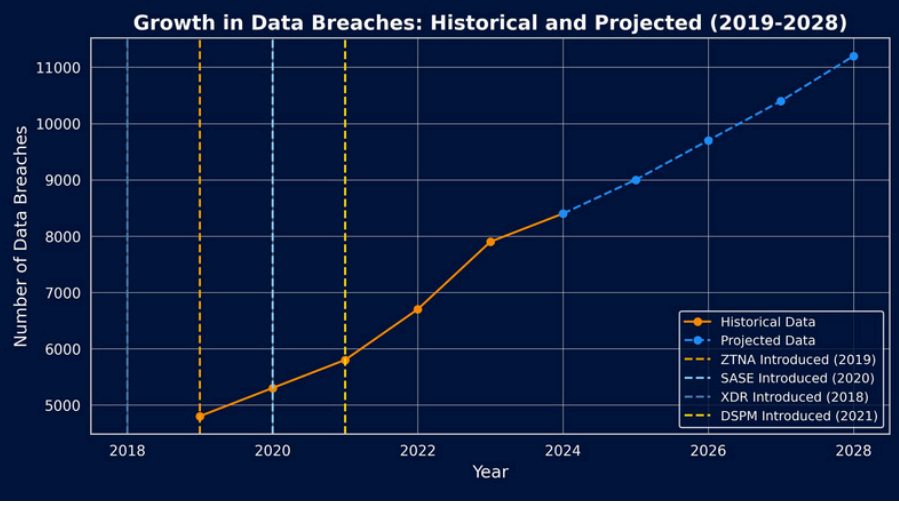
Why Don’t Companies Take Data Loss More Seriously?

Understanding the Rising Threat of Network Breaches and Ransomware

Network breaches and Ransomware attacks are happening daily across all verticals and against both large and small companies, but why? Surely these companies are following the best practise and deploying the latest recommended network security and monitoring? When you map the rise in breaches against the introduction of technology designed to stop them we can see that the traditional approach of perimiter-based security measures is not working to stop or even slow the rate of breaches.



But breaches in the network are only the tip of the iceberg when it comes to the result of a network breach - that’s a whole other level of disruption for a business and is a direct result of the target of those breaches - the data.

Remember a network breach occurs for one of two reasons and one is more likely than the other:

1. **Personal or financial gain**
2. **Distruption**

Personal or Financial gain is the main reason for a network breach - data is now the most valuable asset of a business, that could be anything from personnel information to Intellectual Property and everywhere in between.

How Does the Value of Data Compare to Other Assets?

The value of data is often greater than physical assets, yet many companies still fail to prioritize it accordingly. Let's see how data's worth stacks up against cash, intellectual property, real estate, and other valuable assets:

Data vs. Cash

- Unlike cash, data does not have a fixed face value but can be monetized multiple times.
- Hackers steal data because it can be resold, not just spent once.
- **Example:** The black-market value of stolen credit card details ranges from $10 to $100 per card, but the financial damage caused by fraud can be thousands per incident.
- D**ata Breach Costs:** According to IBM, the average cost of a data breach in 2023 was $4.45 million, far exceeding typical cash thefts.

Verdict: Data is more valuable than cash in terms of resale and impact.

Data vs. Intellectual Property (IP)

- Intellectual Property (patents, trade secrets, proprietary algorithms) is one of the most valuable types of data.
- Companies like Apple, Amazon, and Tesla derive most of their value from proprietary technology rather than physical assets.
- **Example:** The Coca-Cola formula and Google's search algorithm are considered priceless because their secrecy gives these companies a competitive edge.

- When IP is stolen, years of R&D and market advantage can be lost overnight.

Verdict: Data (especially IP) can be more valuable than even patents and trade secrets.

Data vs. Real Estate

- Real estate values are fixed by market forces, whereas data's value can grow exponentially when used effectively.
- **Example:** A prime office space in New York might be worth $50M-$100M, but Facebook's user data alone is valued at hundreds of billions.
- Companies like Airbnb and Zillow do not own real estate, but their data-driven models generate billions.
- When data is lost or breached, companies can lose billions instantly, whereas real estate typically depreciates slowly.

Verdict: Data is more volatile but can be far more valuable than physical real estate.

Data vs. Commodities (Gold, Oil, Bitcoin)

- Oil was historically the world's most valuable resource, but today, data is often called "the new oil" because it fuels business growth.
- Unlike oil, data does not deplete—it can be replicated and resold multiple times.
- Bitcoin (a digital asset) functions similarly—its value is derived from scarcity and security, but data has limitless value potential depending on how it is used.
- **Example:** The market value of data-driven companies like Google, Meta, and Amazon exceeds $4 trillion, surpassing the global oil industry.

Verdict: Data is more versatile and renewable than commodities like gold and oil.

Data vs. Corporate Assets (Machinery, Factories, Equipment)

- Traditional manufacturers rely on physical production, while modern tech giants thrive on data-driven decision-making.
- **Example:** Tesla's self-driving AI data is more valuable than its factories because it dictates the company's future.
- A manufacturing plant may depreciate over time, while data assets can increase in value through analytics and AI.

Verdict: Data can be more valuable than physical infrastructure.

> **Stolen credit card details typically sell for $10-$100 on the dark web, but the financial damage caused per breach can reach thousands or even millions.**
>
> **This makes data breaches highly profitable for cybercriminals and devastating for businesses.**
>
> *Paul German – CEO, Certes*

Data vs. Human Capital (Employees)

- Employees are critical assets, but businesses today make hiring and operational decisions based on data.
- **Example:** AI-driven recruitment platforms use data analytics to optimize hiring, sometimes reducing reliance on human HR managers.
- The biggest companies (Google, Amazon) invest more in data processing and AI automation than in traditional labor.

Verdict: Data amplifies human capital value but, in some cases, can replace it.

- **Data can be replicated, resold, and monetized in ways that cash, real estate, or physical assets cannot**
- **Data breaches cost companies more than physical theft**
- **Businesses today are valued more on their data than their physical assets**

Many companies fail to treat data loss as a major problem due to a mix of overconfidence, misaligned priorities, cost concerns, and a lack of awareness.

Overconfidence in Existing Security Measures

- Many companies believe their firewalls, backups, and cybersecurity tools are enough to prevent data loss.
- Reality: Even with top-tier security, breaches still occur (e.g., Equifax, SolarWinds).

Misunderstanding the True Cost of Data Loss

- Executives often underestimate the financial impact of a data breach.
- **Reality:** Data loss can lead to:
  - Regulatory fines (e.g., GDPR penalties up to 4% of global revenue).
  - Lawsuits from customers and investors.
  - Reputational damage, which can cause long-term business decline.
  - Operational downtime, impacting revenue.
- **Example:** In 2023, a major UK law firm lost sensitive client data, leading to millions in damages and lost trust.

Prioritizing Short-Term Costs Over Long-Term Risks

- Cybersecurity & data protection are seen as costs, not investments.
- Companies may cut budgets for data security to save money, thinking “it won’t happen to us.”

- **Reality:** Data loss can cost millions in recovery efforts, legal fees, and lost customers.
- **Example:** A small U.S. healthcare company skipped security upgrades and suffered a ransomware attack, leading to bankruptcy.

Lack of Awareness at the Executive Level

- C-suite executives often do not understand technical risks.
- Many assume that IT departments alone handle cybersecurity.
- **Reality:** Data protection is a business-wide issue, requiring company-wide training and executive involvement.
- **Example:** Uber's former CISO was convicted for failing to disclose a data breach, showing how executives can be held accountable.

Over-Reliance on Backups

- Many businesses think having backups means they are safe.
- **Reality**:
  - Backups are often outdated or improperly stored.
  - Ransomware attacks can encrypt both primary data and backups.
  - Data leaks & theft are separate issues that backups do not fix.
- **Example**: Maersk, a shipping giant, had to rebuild its entire IT infrastructure after a ransomware attack, despite having backups.

Underestimating Insider Threats

- Many companies assume data loss comes from hackers, ignoring insider risks.

Reality: Data is often lost due to:

- Employee mistakes (accidental deletion, misconfigurations).
- Disgruntled employees stealing or deleting critical data.
- Third-party contractors mishandling sensitive data.

Example: An employee at Tesla tried to leak confidential data but was stopped due to security monitoring.

> **Insider threats are a major cause of data breaches, whether through malicious actions or accidental leaks.**
>
> **Employees with access to sensitive information can unintentionally or deliberately expose critical business data.**
>
> *Simon Pamplin – CTO, Certes*

Poor Regulatory Compliance Understanding

Companies often focus on financial and operational risks but ignore compliance risks.

Reality: Many industries require strict data protection:

- GDPR (EU): Fines for personal data loss.
- CCPA (California): Consumer rights violations.
- HIPAA (Healthcare, U.S.): Heavy penalties for mishandling patient data.
- SEC Rules: Publicly traded companies must disclose cyber risks.

Example: British Airways was fined £20M for failing to protect customer data.

Reactive vs. Proactive Security Approach

Many businesses only act after a breach happens instead of preventing it.

- **Reality**: Companies that invest in proactive data protection (e.g., data-level encryption, access controls, AI-based monitoring) are far less likely to suffer catastrophic data loss.

Conclusion: Why Companies Need to Take Data Loss Seriously

Data loss is not just an IT issue—it's a business-critical risk that can lead to:

- **Legal trouble & fines**
- **Reputational damage**
- **Operational impact**
- **Loss of customers & revenue**
- **Business failure**

A Data-First Security Strategy is required utilizing secure Quantum-based solutions such as DPRM from Certes, where the data itself is always sovereign to the data owner and completely valueless to the attacker. By making the data valueless and not allowing it to be resold or ransomed back, you remove the entire reason for the attack in the first place.

Forward-thinking companies are already following a strategy of "Devalue the Data" to take them off the attackers' target list.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142

sales@certes.ai